CHAPTER 14

プライベート VLAN の設定

この章では、Catalyst 3560 スイッチにプライベート VLAN を設定する方法について説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

この章の内容は、次のとおりです。

（注） プライベート VLAN を設定した場合、スイッチは VTP トランスペアレント モードでなければなりません。第 13 章「VTP の設定」を参照してください。

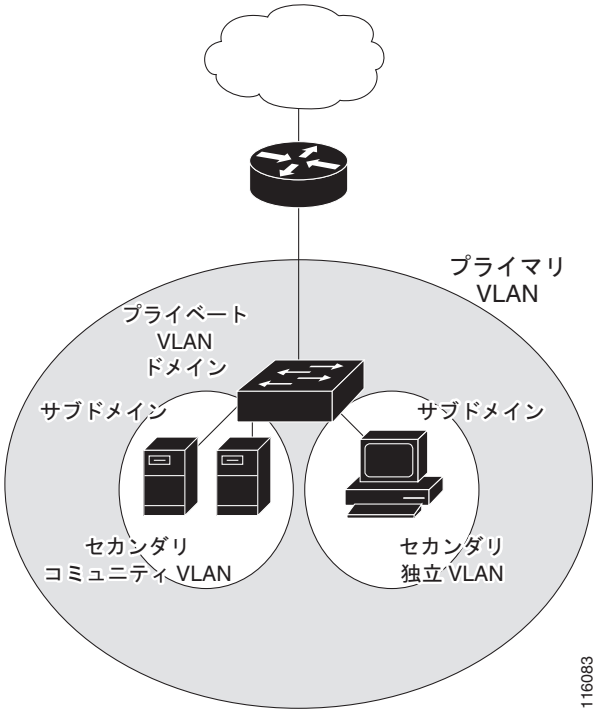
プライベート VLAN の概要

プライベート VLAN 機能は、サービス プロバイダーが VLAN を使用している場合に直面する 2 つの問題に対処します。

- スケーラビリティ：スイッチは最大 1005 のアクティブ VLAN をサポートします。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処でき、サービス プロバイダーにとっては IP アドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。プライベート VLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、*プライマリ* VLAN と *セカンダリ* VLAN のペアで表されます。プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。図 14-1 を参照してください。

図 14-1　プライベート VLAN ドメイン



セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルで相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次の 3 つのタイプがあります。

- 無差別：無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。
- コミュニティ：コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。

（注）　トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN はセカンダリ VLAN であり、コミュニティ ポートから同一コミュニティの無差別ポート ゲートウェイおよびその他のホスト ポートにアップストリーム トラフィックを搬送します。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。レイヤ 3 ゲートウェイは通常無差別ポートを介してスイッチに接続されています。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベート VLAN を使用し、次の方法でエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。プライベート VLAN コンフィギュレーションのセキュリティを保って VLAN の他のユーザがプライベート VLAN に設定されないようにするには、プライベート VLAN ポートのないデバイスを含む、すべての中間デバイス内にプライベート VLAN を設定します。

プライベート VLAN による IP アドレス指定方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

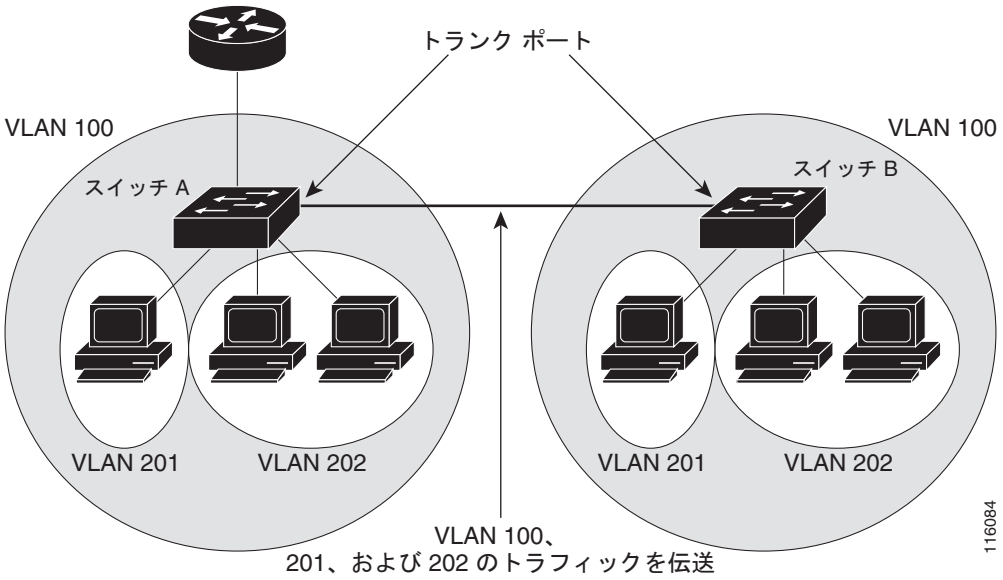
この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ

VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネット アドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のスイッチの PVLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。図 14-2 を参照してください。

図 14-2　　複数のスイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VTP はプライベート VLAN をサポートしないので、レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、これらのスイッチのレイヤ 2 データベースは統合されません。これにより、これらのスイッチにプライベート VLAN トラフィックの不要なフラッディングが発生する可能性があります。

（注） プライベート VLAN をスイッチに設定するときに、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されている場合、デフォルト テンプレートを設定するのに **sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。第 7 章「SDM テンプレートの設定」を参照してください。

プライベート VLAN の他機能との相互作用

プライベート VLAN には、次のように他の機能と相互作用があります。

- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」（P.14-5）
- 「プライベート VLAN と SVI」（P.14-5）

「セカンダリ VLAN およびプライマリ VLAN の設定」（P.14-7）の下にある「プライベート VLAN 設定時の注意事項」も参照してください。

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、ブロードキャストはその VLAN のすべてのポートに転送されます。プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて単一のコミュニティ VLAN 内にルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチでは、スイッチ仮想インターフェイス（SVI）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN を通してだけプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN の設定

ここでは、次の設定について説明します。

プライベート VLAN の設定手順

プライベート VLAN を設定するには、次の手順を実行します。

ステップ 1　VTP モードをトランスペアレントに設定します。

ステップ 2　プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。「プライベート VLAN 内の VLAN の設定および対応付け」（P.14-10）を参照してください。

（注）　VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。

ステップ 3　インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（P.14-12）を参照してください。

ステップ 4　インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」（P.14-13）を参照してください。

ステップ 5　VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」（P.14-14）を参照してください。

ステップ 6　プライマリ VLAN 設定を確認します。

デフォルトのプライベート VLAN 設定

プライベート VLAN は設定されていません。

プライベート VLAN 設定時の注意事項

プライベート VLAN 設定時の注意事項は、次のカテゴリに分けられます。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定を行うときは、次の注意事項に従ってください。

- VTP をトランスペアレント モードに設定します。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。VTP については、第 13 章「VTP の設定」を参照してください。
- プライベート VLAN を設定するには VLAN コンフィギュレーション（config-vlan）モードを使用する必要があります。VLAN データベース コンフィギュレーション モードの場合は、プライベート VLAN を設定できません。VLAN 設定の詳細については、「VLAN コンフィギュレーション モードのオプション」（P.12-7）を参照してください。
- プライベート VLAN を設定後、**copy running-config startup config** 特権 EXEC コマンドを使用して VTP トランスペアレント モード設定およびプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。
- VTP は、プライベート VLAN の設定を伝播しません。プライベート VLAN ポートが必要な各デバイスにプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパニングツリー プロトコル（STP）インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます
- プライベート VLAN を設定すると、スティッキ アドレス解決プロトコル（ARP）がデフォルトでイネーブルになり、レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリはスティッキ ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートのスティッキ ARP エントリには期限切れがありません。

（注） プライベート VLAN インターフェイスの ARP エントリを表示して確認することを推奨します。

IP アドレスが同じでも、MAC アドレスが異なるデバイスを接続すると、メッセージが表示され、ARP エントリは作成されません。プライベート VLAN ポートのスティッキ ARP エントリには期限がないため、MAC アドレスが変更された場合は、プライベート VLAN ポートの ARP エントリを手動で削除する必要があります。

  - **no arp** *ip-addres* グローバル コンフィギュレーション コマンドを使用して、プライベート VLAN の ARP エントリを削除できます。
  - **arp** ip-*address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用して、プライベート VLAN の ARP エントリを追加できます。

- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます（「VLAN マップの設定」（P.31-30）を参照）。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
  - フレームがホスト ポートから無差別ポートにアップストリームで送信される場合は、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - フレームが無差別ポートからホスト ポートにダウンストリームで送信される場合は、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN; VLAN ベースの SPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。

プライベート VLAN ポート設定

プライベート VLAN ポートの設定を行うときは、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定した VLAN に割り当てられたレイヤ 2 アクセス ポートは、VLAN がプライベート VLAN 設定の一部の間は非アクティブになります。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- ポート集約プロトコルまたは Link Aggregation Control Protocol（LACP）EtherChannel に属するポートをプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。
- 誤った設定による STP ループを発生させず、STP コンバージェンスを高速にするために、独立およびコミュニティ ホスト ポートで PortFast および BPDU ガードをイネーブルにします（第 19 章「オプションのスパニングツリー機能の設定」を参照）。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。

- プライベート VLAN 設定で VLAN を削除した場合、VLAN に対応付けられたプライベート VLAN ポートが非アクティブになります。
- デバイスがトランクに接続されていてプライマリおよびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートを別のネットワーク デバイス上に設定できます。

その他の機能の制限事項

プライベート VLAN を設定する際に、他の機能との間で次のような制限があることに留意してください。

（注）　一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。
- Internet Group Management Protocol（IGMP）スヌーピングがスイッチ上でイネーブル（デフォルト）の場合、スイッチがサポートするプライベート VLAN ドメイン数は、20 までです。
- Remote SPAN（RSPAN; リモート SPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。

  SPAN の詳細については、第 27 章「SPAN および RSPAN の設定」を参照してください。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - ダイナミックアクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
- プライベート VLAN ポートはセキュア ポートにはできないので、保護ポートとして設定できません。
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL は、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要があります。スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

（注）　プライベート VLAN の 1 つの VLAN で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、セカンダリ VLAN で学習した MAC アドレスは、プライマリ VLAN で複製されます。元のダイナミック MAC アドレスが削除されるか期限切れになると、複製されたアドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。

プライベート VLAN 内の VLAN の設定および対応付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を行います。

（注）　**private-vlan** コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vtp mode transparent**	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。
ステップ 3	**vlan** *vlan-id*	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan primary**	VLAN をプライマリ VLAN として指定します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 7	**private-vlan isolated**	VLAN を独立 VLAN として指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**vlan** *vlan-id*	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 10	**private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 11	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**vlan** *vlan-id*	ステップ 2 で指定したプライマリ VLAN 用の VLAN コンフィギュレーション モードを開始します。
ステップ 13	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 14	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 15	**show vlan private-vlan** [**type**] または **show interfaces status**	設定を確認します。
ステップ 16	**copy running-config startup config**	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。プライベート VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスペアレント モード設定とプライベート VLAN 設定を保存する必要があります。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。

セカンダリ VLAN をプライマリ VLAN に関連付ける際に、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。
- セカンダリ VLAN とプライマリ VLAN 間の関連付けを消去するには、*secondary_vlan_list* パラメータを指定して **remove** キーワードを使用します。
- このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN と関連付けるには、特権 EXEC モードで次の手順を実行します。

（注）　独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ 3	**switchport mode private-vlan host**	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*	レイヤ 2 ポートをプライベート VLAN に関連付けます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、これにプライベート VLAN ペアを関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
```

```
<output truncated>
```

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。

（注）　独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ 3	**switchport mode private-vlan promiscuous**	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 4	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*	プライベート VLAN 無差別ポートを、プライマリ VLAN と選択したセカンダリ VLAN にマッピングします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 7	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定した場合、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除します。

次に、インターフェイスをプライベート VLAN 無差別ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示します。

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注）　独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *primary_vlan_id*	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して VLAN を SVI として設定します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 3	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングしてプライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interface private-vlan mapping**	設定を確認します。
ステップ 6	**copy running-config startup config**	（任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

（注）　**private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際、構文について次の点に留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN をプライマリ VLAN にマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ VLAN 入力トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

プライベート VLAN のモニタ

表 14-1 に、プライベート VLAN モニタ用の特権 EXEC コマンドを示します。

表 14-1　プライベート VLAN モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インターフェイスのステータスを表示します。
show vlan private-vlan [**type**]	スイッチのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Gi0/1, Gi0/4
10      503       non-operational
```